Identity Document Authentication using Steganographic Techniques: The Challenges of Noise

Juanita Blue
Intelligent Systems Research Centre
Ulster University
Derry, Northern Ireland, UK

Joan Condell, Tom Lunney
Intelligent Systems Research Centre
Ulster University
Derry, Northern Ireland, UK

***Abstract*— The term 'steganography' encapsulates the practice of secretly embedding data into digital mediums including video, image and audio files. Although steganography is often associated with nefarious activities, conceptually it asserts several characteristics that render it useful in contemporary security applications. Not just a mechanism for criminals to communicate secret information over a digital channel, steganography is also used as a legitimate method of ensuring integrity of digital media artefacts and for identification of same. This application of steganography allows for identification images storing additional information to verify both the identity of the subject as well as the authenticity of the image.**

Developed methods of steganography invoke various spatial domain techniques that are successful in covertly concealing data within 'innocent' carrier images. The techniques include linear methods such as those which replace the least significant bit (LSB) of the bytes in an image and frequency domain methods including discrete cosine transform (DCT), discrete wavelet transform (DWT) and discrete Fourier transform (DFT). The success of a steganographic algorithm is hinged on the method's ability to successfully embed data, so that the data remains concealed within a carrier image; and also to successfully extract the same data uncorrupted. Often modern image coding formats include lossy compression in the frequency domain; this can result in data loss, corruption and noise within the image when carrier images are re-encoded. To ensure data extraction is successful, error correction functions must be invoked to counteract noise and ensure embedded data is extracted without any loss or corruption.

In exploring steganographic software, the functionality and reliability of a novel steganographic application '*Intelligent Identity Authenticator*' (IIA) was assessed. IIA invokes the use of steganography to conceal real-time identity information within images on identity cards. The functionality of IIA is based on a unique algorithm that utilizes DWT to embed a string of characters within an identity image. When data is extracted, it provides a link to further documentation relating to the data subject, allowing for verification of the claimant's identity and authenticity of the identity card.

The embedding and extraction functions executed by IIA were found to be mostly reliable, except where data had been embedded within a carrier image that was characterized by a large proportion of black pixels. In these cases, the extracted data string experienced significant loss and corruption, thus preventing access to the identity verification documentation. This paper explores the potential cause of this specific corruption and discusses extensive testing conducted on control images. The results are analysed to identify an improved solution that could rectify the issue, with an aim to improving both the functionality and reliability of the IIA system.

Keywords—steganography; image processing; noise; error-correction; authentication

I. INTRODUCTION

A. Identity Theft and IdentityVerification

Advancements in technology and increased dependence on digital sharing of information have presented challenges in protecting the integrity, confidentiality and availability of personal data [1]. One such challenge is the rise in identity theft, where perpetrators use the identities of others for nefarious purposes and essentially to violate the law [2]. Identity theft is "…the misuse of another individual's personal information to commit fraud" [3] and generally occurs in two stages; illegally obtaining personal information relating to the identity of an individual and using this information to create a fake identity through false or fraudulent documentation [4].

Counterfeit identity cards have become increasingly commonplace, thus, authentication and verification of identity documentation has become a salient issue with the surge in incidents of identity theft [5]. When individuals identify themselves, they are making a claim of identity based on a variety of different credentials including name, birthdate, birthplace, address, education and professional information, amongst others. However, these claims alone do not authenticate identity; supportive evidence is required to verify that the identification document and the information contained therein are valid and the identity of the individual is verified [6]. To counteract counterfeit documentation, theft resistant authentication mechanisms must be built into identity cards to prove the identity assertions that are made, and to protect the true and legitimate identity [5].

To achieve this end, industry invokes various types of security and verification features within identity cards ranging from tamper-proof laminates to holograms and more advanced features such as ultraviolet ink and microprint [7][8][9][10]. Although these features verify the authenticity of the card itself, they do not verify the identity presented on the card. To do so would require the card to link to a real-time central repository that verifies the individual is authorized to possess the identity card itself, thus verifying the link between the card and the card-holder [11].

B. Authentication via Steganographic Techniques

Steganography is the practice of secretly embedding data into a digital medium referred to as a 'carrier' [12]. An effective steganographic scheme should possess the following desired characteristics:

- Secrecy: The hidden data cannot be extracted from the carrier image without use of a specialist algorithm or tool, in addition to knowledge of a secret key [13][14].
- Imperceptibility: Embedded data should remain covert with no discernible changes to the carrier image [13].

- High capacity: The carrier image should be capable of embedding a large amount of data [13].
- Resistance: The embedded data should be robust and capable of carrier image changes such as lossy compression and cropping [13].
- Accurate extraction: Extracted data should be intact, suffering no loss or corruption [13].

If the aforementioned criteria are met, the use of steganography in identification cards presents the potential capacity to verify the identity of the individual and also the authenticity of the card itself.

A proven steganographic application called IIA was examined for functionality and reliability. The application operates by embedding data in the form of a filename and link into identification images. Upon data extraction, the link provides access to a real-time central digital repository. The repository contains documentation that verifies and authenticates the identity card detail.

Extraction failures experienced in initial tests conducted on IIA indicated that the application initially failed to meet the aforementioned criteria. In its current form, IIA would not be considered a viable solution for intelligent identity authentication unless the embedded data was successfully extracted with each use. This paper explores the functionality and reliability issues that were encountered when the scheme was employed. It aims to identify the cause of the malfunction and offer potential solutions that will result in a fully functional, reliable and effective scheme that allows the application to operate successfully as an intelligent identity authenticator.

II. BACKGROUND

This section provides a background for the concepts associated with identity authentication and the features that support it. It also gives a brief explanation of various methods of steganography including affiliated topics such as colour models, image noise and error correction functions. Lastly, it provides an outline of the core functionality of IIA and the challenges that were encountered when invoking the application to embed verification data into identity images. Collectively, these explorations justify the extensive tests that were conducted in a bid to identify the origin of corrupted extractions.

A. Identity Cards: Security Levels & Features

Fraudulent identities and their supporting documentation are much coveted by individuals and groups who wish to commit various types of crime. In an attempt to suppress the ability of such parties from successfully producing counterfeit identity cards that appear realistic and thus verify false or stolen identities, various security features are incorporated into modern identity cards. These features seek to verify the authenticity of the card and confirm the identity of its holder is real and the detail is correct. Security features are often included in both commercially marketed and official/government issued identification cards in a bid to stamp out fraudulent documentation. Table I describes the levels of security, the essential attributes at each level and also provides examples of the features each encompasses [10][15][16][17].

Table I. Identification Document Security Features

Security Level	*Attributes*	*Examples*
Level 1: Overt	• Basic requirement • Lowest level security • Visual verification via discernable features • Overtly printed features • Characterised by method of production • Physical additives to card substrate and laminate	• Visible watermarks • Holograms • Security designs • Fine printing • Fibres • Security laminates • Overt biographic data • Embossed ridges
Level 2: Covert	• Compliment level 1 features • Not readily perceivable • Requires basic specialist tools to capture, register and authenticate data (lighting, magnification)	• Smart chips • Contactless chips • Magnetic Stripes • Radio Frequency ID • UV Ink • Microprinting
Level 3: Forensic	• Optimum security • Complex & Specialized • Visually perceivable data combined with secret data • Requires specialist forensic tools to capture, register and authenticate data (unique algorithms) • Optimal schemes link to a real-time digital central repository to verify and expand on overt/covert detail	• Steganography • Barcodes • Qode, • QR Code • Nexcode • SecureText™

In combination, features from these levels provide a comprehensive assurance of validity and authenticity of identification cards and related documents. The categorised features are incorporated to protect identity information on crucial documents to ensure originality and accuracy of the identities they represent [15].

Level 1 (overt) security features provide the advantage of a simple and swift cursory visual verification of identity information and document authenticity without specialist tools, these features are easily tampered with or copied. [15]. However, these features alone do not provide adequate security; advancements in commercially available card production equipment have facilitated improved fraudulent replication.

Level 2 (covert) security features theoretically prevent alteration to the data concealed within the identity card [15]. The data capacity of each mechanism is constrained by the feature's memory size and technical capabilities [10]. Recent technological advancements have resulted in breaches of these features and as such may no longer be considered entirely secure.

Level 3 (forensic) security features provide security and integrity of information from a surface level to that which is infinitely complex and specialized [15]. They facilitate centralised and forensic security controls which are applied in combination with localised and limited security features [15][16]. Centrally retrieved original data can reveal discrepancies in documentation and expose those that are fraudulent. Forensic features have been endorsed by the United Nations Office on Drugs and Crime (UNODC) and the United Nation Global Initiative to Fight Human Trafficking (UN.GIFT) [11][18]. The Vienna 2008 Forum ratified that various machine readable code implementations are difficult to

falsify due to a central and protected source database with appropriate access authorisation implementations (Article 12, Legislative Guide for the Implementation of the Protocol to Prevent, Suppress and Punish Tracking in Persons) [18].

Examination of identity document security features has categorized the function offered by IIA as a forensic feature. The embedded data is concealed from plain sight, requires a special digital tool/algorithm to extract and connects to a central repository that verifies and expands upon the information that is overtly displayed on the identification card.

B. Color Space Models

A color space model is an abstract mathematical model which simply describes the range of colors as tuples of 3 or 4 values or color components. Each color space is an elaboration of the coordinate system and sub-space, where every color in the system is represented by a single dot known as a pixel. A typical example is the *Red Green Blue* (RGB) model, currently the most popular implementation as it is compatible with common image file formats such as *Graphics Interchange Format* (GIF), *Portable Network Graphics* (PNG) and *Joint Photographic Experts Group* (JPG). RGB assigns a value between 0 and 255 to each of the red, green and blue bytes that define each pixel. In this model 0 is the darkest and 255 is the lightest, thus the combination of values produces a specified colour. With this model R=0,G=0,B=0 produces black and R=255,G=255,B=255 produces white.

Alternate colour space models are also available, these include *Cyan, Magenta, Yellow and Key* (CMYK), and YCbCr, where Y is the luma component, Cb is the blue-difference chroma component and Cr is the red-difference chroma component. Often to invoke complex steganographic techniques, the original colour space model of an image may need to be converted one or more times to embed data. This is achieved by applying specific mathematical functions to pixel byte values.

C. Steganographic Techniques

Various forms of steganography have been invoked for thousands of years, where information and 'secrets' are hidden in plain sight. In the digital era, steganographic techniques have adapted to utilize digital mediums such as audio, video and images. In image steganography, data can be stored in the form of ASCII code at binary level in carrier images. Pixel byte values that define colour and luminance are manipulated to store binary representations of the secret message data bit by bit.

One of the simplest steganographic techniques is the LSB method where the smallest bit (value of 1) of the red, green or blue byte is altered to store the necessary value (1 or 0). This has no perceivable impact on the colour or intensity of the image [19]. This method can be further extended to alter the values of all the bytes, or utilize a random number generator to randomly distribute alternate bit values, rather than operating in a sequential linear manner [20].

Frequency domain techniques such as DCT and DWT involve significantly more complex processing to embed data. In the frequency domain, bit representations of information can be inserted into coefficients of image transforms such as DFT, DCT and DWT [19]. These techniques have proven to be more robust for embedding data, especially when the carrier image undergoes common processing operations and lossy compression [20].

The rate of change in pixel values across an image defines the spatial frequency. The frequency domain identifies how much the average colour values alter from one pixel to the next. This allows images to be represented as complex waves that can be decomposed into standard waves of different frequencies. Coefficients are the weightings assigned to standard waves depending on their contribution to complex waves [20].

High spatial frequency is described as the areas of an image in which the colour varies rapidly. Low frequencies are described as areas where there is no variation. The different frequencies are overlaid to produce an image and the frequency coefficients are used to determine the strength of a particular frequency in a specific section of the image [19]. This allows for separation and removal of information that is high frequency and beyond human perception. Frequency components with minimal coefficients are discarded, leaving only the significant contributors to the image [20]. DCT transforms pixel values representing the spatial domain into representations in the frequency domain. This can be executed repeatedly with an objective of compressing image data so it can be stored or transmitted and later decompressed to reform the original image [19].

DWT is any wavelet transform for which the wavelets are discretely sampled. Wavelet transforms are based on small waves of varying frequency and limited duration. The Haar DWT transform uses square waves to approximate an original function. The pixels are scanned in two operations; horizontally and vertically where addition and subtraction functions are performed on neighboring pixels. Sums and differences from each scan are stored on the left and right respectively (horizontal scan), and the top and bottom respectively (vertical scan). The pixel sums represent the low frequency element (L), while the pixel differences represent the original high frequency element (H). The result is 4 sub-bands denoted as LL, HL, LH, and HH. As depicted in Figure 1, the process can be reiterated to produce additional sub-bands. The LL sub-band appears most similar to the original image [19].

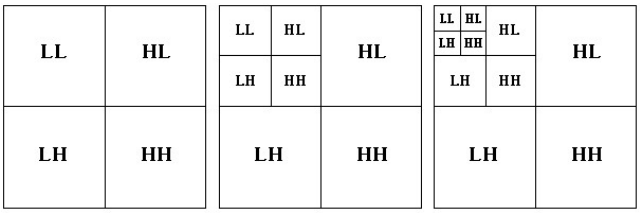

Fig. 1. DWT Sub-bands

D. Image Noise

Digital images are prone to a variety of noise types, where a pixel does not match those surrounding it. Image noise is often the source of distortion or poor quality images and can be introduced in several ways dependent on the invoked image creation technique [21]. Various types of noise produce distortion as described in Table II [22].

Table II. Types of Image Noise

Noise Type	***Result***	***Appearance***
Photoelectronic	• Photon Noise • Thermal Noise	• Granular Appearance
Impulse	• Salt Noise • Pepper Noise • Line Drop	• White Speckles • Black Speckles • Black Lines

Noise Type	*Result*	*Appearance*
Structured	• Periodic, Stationary • Periodic, Nonstationary • Aperiodic • Detector Striping • Detector Banding	• Phased Repetitive Lines • Appearance of Ridges • Stripes • Pixelated Appearance

E. Error Correction Functions

Modern image coding formats often include lossy compression in the frequency domain where data beyond human perception is discarded to reduce the size of the digital file. A chief characteristic of an effective steganographic technique is the ability to maintain the integrity of data stored in a carrier file, even if that file is subject to filtering, resampling, cropping, or lossy compression. Often re-encoding following these processes results in lost and corrupted data where bits in the embedded data string are deleted, replaced and inserted [23].

Data is transmitted in a bit-stream over channels where the presence of noise is common. The noise may alter messages causing the received message to differ significantly from that which was originally sent, resulting in low reliability [25]. Coding theory addresses the altered result of data transmitted across a noisy channel, and aims improve reliability by converting error-ridden received messages back to their original error-free form [24].

F. Operation of Intelligent Identity Authenticator

Examination of the IIA algorithm revealed that the application embeds secret data in identity card imagery by executing the following sequence of steps:

The application accepts user input arguments in the form of a potential carrier image file (PNG or JPG) and a PDF file that documents a subject's personal information. The carrier file and PDF documents are stored in a remote digital central repository. The carrier image is processed by converting the RGB model to the YCbCr model using a pre-defined mathematical equation. DWT is invoked to split the colour planes into Y, Cb and Cr. The link to the PDF document is converted to a binary string and embedded in lower left hand corner of the Y plane of the image.

To extract the embedded data, the same process is reversed, with an additional step for error-correction. When the link to verification documentation is successfully extracted, the central digital repository is accessed and the supporting PDF documentation may be viewed.

G. Functionctionality & Reliability Testing

Basic-level functionality and reliability tests were conducted to ensure IIA operated effectively. This testing resulted in a large number of failed extractions. In a bid to ascertain the source of the failures, further simple tests were conducted. Analysis of results identified basic system requirements such as document compatibility and filename attributes and length. Correct processing of input documents only occurred with PNG or JPG formats and filenames twelve characters in length. Subsequent tests adhered to the aforementioned conditions and although the rate of failure was significantly reduced, the system still experienced a substantial number of unexplained extraction failures.

With consideration for the defined effective steganographic scheme criteria, it was concluded that IIA could not be considered functional or reliable and hence was not an effective scheme. During the later tests it was observed that specific images resulted in failed extractions. On closer inspection, it was identified that problematic image files all shared a common characteristic in that they all contained a large amount of black.

Based on this premise, it was hypothesized that excess black pixels may causing the unexplained extracted failures. Consequentially, subsequent tests were focused on images that were comprised of large black pixel blocks. As depicted in Figure 2, custom images were created to include large areas of black pixels in specific areas of carrier images.

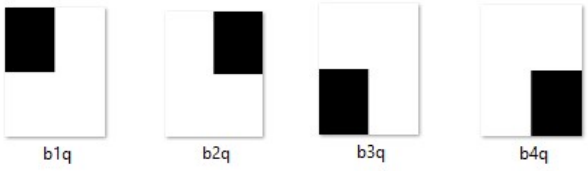

Fig. 2. Various testing positions of large blocks of black pixels

These tests resulted in two observations; large amounts of black pixels indisputably resulted on corrupted data extractions and the specific problematic area was the lower left hand corner of the image. While extractions from images b1q, b2q and b4q (depicted in Figure 2) were successful, all attempted extractions from image b3q, also referred to as the third quadrant, resulted in a corrupted data string. Figure 3 pinpoints the location of each of the quadrants.

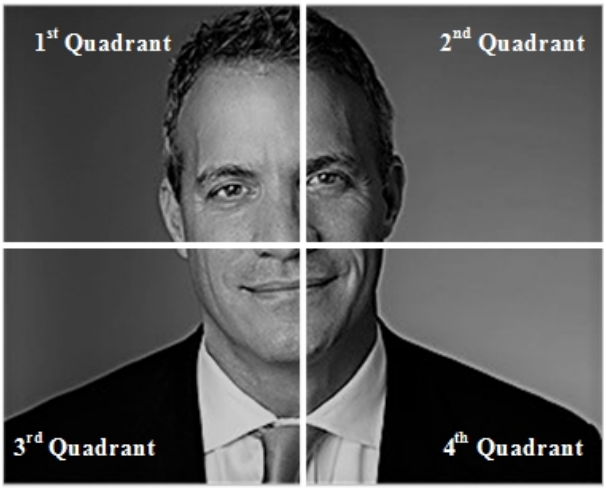

Fig. 3. Defined Image quadrants

It was suspected that the third quadrant may be the area of the carrier image where IIA embedded data. Inspection of the IIA source code confirmed this hypothesis, thus providing explanation for the difficulty experienced with this specific area of the carrier image. However, this discovery did not reveal why this complication was explicitly confined to pixels that were black, having an RGB value of (0,0,0).

Corruption of the embedded data caused by excess black pixels in the third quadrant had the potential to render IIA useless an as effective steganographic scheme for intelligent identity authentication as often identity images depict individuals wearing black. In such cases this would result in the inclusion of large amounts of black pixels in the third quadrant. These results prompted further in depth testing with an aim to identify the root cause and potentially identify a viable solution

to improve the functionality and reliability of IIA, so that it may be considered an effective steganographic scheme.

III. METHODOLOGY

This section describes the testing methods invoked to assess the extent of the impact of black pixels in the third quadrant.

A. Black Pixel TestingMethodology

Due to corrupted data extractions, IIA was unable to meet defined functional requirements, as the system was attempting to access the digital central repository with erroneous links. Tests had concluded that the redundant links experienced character omissions and replacements; furthermore, in extreme cases, no data was extracted at all. Identification of the extraction difficulties associated with black pixels located in the third quadrant warranted further examination of the steganographic algorithm and concentrated testing. A plan was formulated to conduct the following tests:

- Colour Testing: Assess if large blocks of alternate colours in the third quadrant also resulted in failed extractions.
- Gradual Black Pixel Increase Testing: Assess the algorithm's tolerance of black pixels within the third quadrant. Aim to identify specific rows and columns where black pixels become problematic. Potentially identify an acceptable ratio of black pixels.
- Almost Black Pixel Testing: Assess if large blocks of almost black pixels (R=1,G=1,B=1) also negatively impact the extraction process.
- Link Corruption Testing: Convert data strings to binary representations to identify any patterns of corruption present in the extractions, inclusive of data string position, corruption type and consistent character replacements.

B. Image Building

To allow for controlled testing and detailed inspection of image attributes and data string corruption, a custom Java application was developed to construct images. This application was designed to conduct the following:

- Construct images with desired black/colour dispersion
- Identify the total number of pixels in an image
- Identify the black pixel count and coordinates
- Calculate the percentage of black pixels

C. Filename Strings

To aid identification of data corruption patterns, PDF documents were renamed with strings such as 0123456789ab.pdf and abcdefghijkl.pdf where the original string position of characters could be easily ascertained. This would simplify result comparison and analysis when testing was concluded.

IV. RESULTS

This section describes the results of extensive testing previously discussed in Section III.

A. Colour Testing

Control images were constructed that constituted pixels with identical RGB values. The colours chosen for testing were black, white, orange and dark grey. The results in Table III clearly establish that excess black pixels exclusively result in extraction failures. All extraction attempts using alternate colours were successfully executed.

Table III. Colour Testing

Pixel Colour	*Successful Extraction*
Black	✘
White	✓
Orange	✓
Dark Grey	✓

B. Gradual Black Pixel Increase Testing

A series of control images were constructed that initially consisted of a small block of black pixels in the third quadrant that did not impact on the successful extraction of the embedded data string. Each subsequent image increased the black pixel count by increments of 100,000. As depicted in Table IV, with each increment, the number of characters that were correctly extracted in the correct position was reduced, eventually resulting in no successful extraction of any embedded characters.

Table IV. Correct Character Extraction

Black Pixel Count	*Correct Character Extraction*							
15000	12	12	12	12	12	12	12	12
115000	10	10	10	10	10	10	10	10
215000	8	8	8	8	8	8	8	8
315000	5	6	6	5	5	6	5	6
415000	5	3	4	4	5	5	3	4
515000	4	2	3	1	4	3	2	1
615000	4	0	2	1	4	2	2	1
715000	3	0	1	0	2	1	1	0
815000	2	0	0	0	1	0	0	0
915000	0	0	0	0	0	0	0	0

C. Almost Black Pixels

Images with identical pixel counts to those above were constructed; however, instead of defining the pixel values as black (*R=0,G=0,B=0*), the values were defined as 'almost black (*R=1,G=1,B=1*). Tests conducted on these images resulted in continued successful extractions, where the 'almost black' pixels were continually incremented until they filled the entire image. The minor manipulation of the pixel byte values successfully altered functionality of the steganographic algorithm.

D. Extracted String Degradation

The original and extracted data strings were converted to binary representations in order to assess if any consistent patterns of degradation could be identified. Each character was converted to an eight bit byte, resulting in ninety-six bits for each twelve character string. This testing included analysis of the position of bits that were commonly altered with each increase in the number black pixels. The results conclusively identified that near identical bit positions were

suffering alteration with each increased black pixel increment. Clear patterns were identified where the original link began to degrade at binary level, continuing with the alteration of more bits until eventually the original bit string was unrecognizable when compared to that which was extracted. To summarise, the results of this testing confirmed that the excess black pixels in the third quadrant were causing individual bits to be converted from 0 to 1 or vice versa.

V. CONCLUSION

The results allowed for the establishment of two hypothesis:

1. The IIA steganographic algorithm identified excess black pixels in the third quadrant as 'noise'.
2. The invoked error-correction function within the algorithm was over-compensating for the excess black pixels and thus, over-correcting at binary level.

These conclusions indicated that the error-correction function invoked was incompatible with this type of steganographic method. Whilst the error-correction function was over-compensating for black pixel noise, IIA could not be considered an effective steganographic scheme that would allow for intelligent identity authentication.

The 'Almost Black' pixel testing that had been conducted illuminated a swift and easy solution to the data string corruption issue. The steganographic algorithm was altered to convert all black (*R=0,G=0,B=0*) pixels within the image to almost black (*R=1,G=1,B=1*) pixels prior to embedding of the data string. This resulted in no visually perceivable alteration to the image. Subsequent tests confirmed that all images allowed for successful extraction of embedded data without corruption. This allowed for IIA to meet the criteria required and be considered 'an effective steganographic scheme'.

Further work will include experimentation on alternative error-correction functions with IIA; to assess and identify types of error correction functions which are most appropriate for varying types of steganographic techniques.

REFERENCES

[1] A. Asrani , V. Koul and R. Khot , "Review of Network Steganography Techniques" Thadomal Shahani Engineering College, Mumbai, Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-12, ISSN: 2454-1362, 2016

[2] K. Saunders and B. Zucker, "Counteracting Identity Fraud in the Information Age: The Identity Theft & Assumption Deterrence Act", Jnl Intern. Review of Law, Comp. & Technology,Vol 13, Issue 2, 1999

[3]] A. R. Gonzales and D.P. Majoras, "Combating Identity Theft: A Strategic Plan", Office of the President: U.S. Depart. of Justice, 2007

[4] G. R. Gordon, N.A. Willox Jr., D.J. Rebovich, T.M. Regan, and J.B. Gordon. "Identity Fraud: A Critical National and Global Threat", Journal of Economic Crime Management, pp. 1-48, 2004

[5] A. Klenk, H. Kinkelin, C. Eunicke, G. Carle, "Preventing identity theft with electronic identity cards and the trusted platform module", ACM, EUROSEC '09 Proceedings of the Second European Workshop on System Security, pp. 44-51, Nuremburg, Germany, March 2009

[6] C. Bennett and D. Lyon, "Playing the Identity Card: Surveillance, Security and Identification in Global Perspective", Routledge, Oxon, pp. 3-4, 2008

[7] V. Martínez, L. Encinas, A. Muñoz, M. Mariño, D. Guardeño, "A comparative study of three Spanish eGoverment smart cards" Log Journal of the IGPL 2017; Vol. 25, Issue 1, pp. 42-53, August 2016

[8] P. Di Lazzaro, S. Bollanti, F. Flora, L. Mezi, D. Murra, A. Torre, F. Bonfigli, R. Montereali and M. Vincenti, "Invisible marking system by extreme ultraviolet radiation: the new frontier for anti-counterfeiting tags", IOPScience Publishing Ltd/Sissa Medialab SRL, Jnl Instrumentation, Vol11, 4th Intern Confer Frontiers in Diagnostics fix Technologies (ICFDT4), July 2016

[9] D. Lushnikov, A. Zherdev, S. Odinokov , V. Markin and A. Smirnov, "Experimental study of the method of recording color volume security holograms on different photosensitive materials on the base of the diffuser with a narrow indicatrix of laser radiation", Proc. SPIE 10022, Holography, Diffractive Optics, and Applications VII, 100221S, Beijing, China, October 2016

[10] The Council of the European Union, "PRADO Glossary (013) Technical terms related to security features and to security documents in general", Directorate-General Justice/ Home Affairs, Visas and Borders (DGD 1A) Brussels, Belgium, Europe, 2015

[11] United Nations Office on Drugs and Crime Division for the Treaty Affairs, "Legislative guides for the implementation of the United Nations convention against transnational organized crime and protocols thereto", United Nations, New York, V.04-50413,Vienna International Centre, Vienna, Austria, 2004

[12] A. Chaddad, J. Condell, K. Curran and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier, Signal Processing, Volume 90, Issue 3, pp 727–752, March 2010

[13] K.P.Adhiya and Swati A. Patil, "Hiding Text in Audio Using LSB Based Steganography" in Information and Knowledge Management Vol. 2, No.3, 2012

[14] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf, "Modeling the Security of Steganographic Systems", Information Hiding, Lecture Notes in Computer Science, Vol. 1525 , pp 344-354, November 1998

[15] A. Hodgson and S. Simske, "Challenges in Security Printing", NIP & Digital Fabrication Conference, International Conference on Digital Printing Technologies. Society for Imaging Science and TechnologyPages, pp. 148-152, 2013

[16] ITW Security Division, "Document Security Begins with Expert Design", (online) http://www.itwsecuritydivision.com/security-technology/document-security, 2017

[17] Datacard Group, "Card durability and security supplies: Virtual Edge-to-Edge Protection for Secure ID Programs", SG6-6000, 2006

[18] United Nations Global Initialtive to Fight Himan Trafficking, "017 Workshop: Technology and Human Trafficking", The Vienna Forum to fight Human Trafficking, UN.GIFT B.P.:017, February 2008

[19] S. Katzenbeisser and F. Petitcolas, "Information Hiding techniques for steganography and digital watermarking", Artech House, Boston, pp.29

[20] K. Bailey, K. Curran and J. Condell, "Evaluation of pixel-based steganography and stegodetection methods", Volume 52, 2004 - Issue 3, pp. 131-150, 2004

[21] J. Russ and F. Neil, "The image processing handbook", Seventh edition, CRC Press, Boca Raton, FL, pp. 33, 2016

[22] R. Schowengerdt , "Remote Sensing: Models and Methods for Image Processing", Second Edition, Department of Electrical & Computer Engineering, University of Arizona, Academic Press, 1997

[23] J. Keller and J. Magauer, "Error-correcting Codes in Steganography", FernUniversitat Hagen, ARCS'06, 19th International Conference on Architecture of Computing Systems, Workshop Proceedings, March 2006

[24] I. Reed, "Polynomial Codes over Certain Finite Fields". Journal of the Society for Industrial and Applied Mathematics (SIAM) 8 (2): 300–304, 1960

[25] F. Ishengoma, "The Art of Data Hiding with Reed-Solomon Error Correcting Codes", Computer Engineering and Applications, The University of Dodoma, Tanzania, International Journal of Computer Applications (0975 – 8887) Volume 106 – No. 14, November 2014.